IN THE CLAIMS

Please amend claims 1, 18, 41, 49, 57, 71 and 72 as indicated below

The listing of claims below will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A digital communication system to denote confidentiality of a digital communication comprising:

~~a processor; and,~~

a first memory containing a program executable by ~~the~~ a processor to:

attach a privileged attribute to a digital communication; and

create a privileged distribution list of at least one intended recipient and associate the privileged distribution list with the digital communication; and

a second memory containing a program executable by a processor to:

restrict access to the privileged digital communication to the at least one intended recipient according to the privileged distribution list associated with the digital communication;

restrict routing of the privileged digital communication to the at least one intended recipient according to the privileged distribution list associated with the digital communication; and,

store the privileged digital communication in a segregated location for privileged digital communications on a data storage device.

2. (Original) The communication system of claim 1, wherein the at least one intended recipient is a plurality of intended recipients.

3. (Previously Presented) The communication system of claim 1 further comprising:

a mail server; and,

a segregated server housing the segregated location for privileged digital communications;

2

wherein the program is further executable to send a copy of the communication to the segregated server.

4. (Original)   The communication system of claim 3, wherein the copy is sent as a blind carbon copy.

5. (Previously Presented)   The communication system of claim 1 wherein the segregated location for privileged digital communications is divided by a common characteristic of the digital communication, the common characteristic including:

      a sender of the digital communication;

      a recipient of the digital communication; and,

      a department of a corporation using the system.

6. (Previously Presented)   The communication system of claim 1 wherein the program is further executable to configure access rights to the digital communication and to enforce said access rights by managing access to the digital communication and controlling the manipulation of its contents.

7. (Original)   The communication system of claim 6 wherein the access rights include:

      forwarding of the communication;

      replying; and

      replying with copies to pre-selected recipients.

8. (Original)   The communication system of claim 6 wherein the communication includes an address portion and a content portion, and wherein the access rights further include:

      allowing copying of the contents of the communication; and

      allowing cutting the contents of the communication out of the communication and pasting the cut out contents into another location.

3

9. (Original)   The communication system of claim 1 wherein the program is configured to execute automatically and attach the privileged attribute to particular communications according to predetermined selection criteria.

10. (Original)   The communication system of claim 1 further comprising a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication.

11. (Original)   The communication system of claim 10 wherein the user acknowledges the confidentiality notice by clicking on a GUI button.

12. (Original)   The communication system of claim 1 wherein the privileged digital communication is encrypted.

13. (Original)   The communication system of claim 1 wherein the program further comprises a server object and a client object.

14. (Original)   The communication system of claim 13 wherein the client object is configured to attach the privileged attribute, create the privileged distribution list and send the privileged communication to the server object.

15. (Original)   The communication system of claim 13 wherein the server object restricts access and routing of the digital communication and stores the communication in the segregated location.

16. (Original)   The communication system of claim 13 wherein the client object is a plug-in to a pre-existing communication system.

17. (Original)   The communication system of claim 1 further comprising a second segregated location residing on a client device.

18. (Currently Amended)   A digital communication system for denoting confidentiality of a digital communication comprising:

a processor; and,

a memory containing a program executable by the processor to÷ attach an executable module to a digital communication, the executable module constructed and arranged to:

create a privileged distribution list of intended recipients of the digital communication to which it is attached;

restrict access to the digital communication to which it is attached to the intended recipients; and

restrict routing of the digital communication to which it is attached to the intended recipients.

19. (Original)   The communication system of claim 18 wherein the program is further executable to configure access rights to the digital communication and to enforce said access rights by managing access to the digital communication and controlling the manipulation of its contents, wherein the access rights include:

allowing forwarding of the communication;

allowing replying; and

allowing replying with carbon copies to pre-selected recipients.

20. (Original)   The communication system of claim 18 wherein the communication includes an address portion and a content portion, and wherein the access rights further include:

allowing copying of the contents of the communication;

allowing cutting the contents of the communication out of the communication and pasting the cut out contents into another location;

21. (Original)   The communication system of claim 18 wherein the program is configured to execute automatically and attach the executable module to particular communications according to predetermined selection criteria.

22. (Original)   The communication system of claim 18 further comprising a confidentiality notice that is displayed to a user and acknowledged by the user before displaying the privileged communication.

23. (Original)   The communication system of claim 18 wherein the privileged digital communication is encrypted.

24. (Original)   The communication system of claim 18, wherein the program further comprises a server object and a client object.

25. (Original)   The communication system of claim 23 wherein the client object is configured to attach the executable module, and send the privileged communication to the server object.

26. (Original)   The communication system of claim 23 wherein the server object restricts access and routing of the digital communication and stores the communication in a segregated location.

27. (Original)   The communication system of claim 23 wherein the client object is a plug-in to a pre-existing communication system.

28-40. (Canceled)

41. (Currently Amended)   A method for creating an attorney-client privileged digital communication comprising the steps of:

 creating an electronic communication;

 marking the communication privileged with a privileged attribute;

 storing the communication in a segregated location for privileged digital communications on a data storage device;

 configuring access rights to the digital communication and associating a privileged distribution list with the digital communication; and,

 enforcing said access rights by managing access to the digital communication and controlling the manipulation of its contents based upon the associated privileged distribution list;

wherein the access rights include:

      forwarding of the communication;

      replying; and

      replying with copies to pre-selected recipients.

42. (Original) The method of claim 41 wherein the communication includes an address portion and a content portion, and wherein the access rights include:

      copying of the contents of the communication;

      cutting the contents of the communication out of the communication and

      pasting the cut out contents into another location.

43. (Original) The method of claim 41 further comprising automatically attaching the privileged attribute to particular communications according to pre-determined selection criteria.

44. (Original) The method of claim 41 further comprising:

      displaying a confidentiality notice to a user; and,

      requiring acknowledgment by the user of the confidentiality notice before displaying the privileged communication.

45. (Original) The method of claim 41 further comprising applying an encryption technique to the digital communication.

46. (Original) The method of claim 41 further comprising the steps of:

      creating a blind carbon copy of the digital communication;

      sending the blind carbon copy to a segregated server wherein the segregated location resides on the segregated server.

47. (Original) The method of claim 41 further comprising dividing the segregated location by a common characteristic of the digital communication, the common characteristic including one or more of:

      a sender of the digital communication;

a recipient of the digital communication; and

a department of a corporation.

48. (Previously Presented)   The method of claim 41 further comprising the steps of:

creating a second segregated location on a client device;

storing a copy of the digital communication on the second segregated location for privileged digital communications.

49. (Currently Amended)   A method for creating a digital communication protected by privilege comprising the steps of:

creating an executable module constructed and arranged to instruct a computer, according to an associated privileged distribution list, to restrict access to the communication to which the executable module is attached in order to maintain the application of the privilege;

attaching the executable module to the communication, whereby the executable module instructs the computer to restrict access to the communication according to the associated privileged distribution list.

50. (Original)   The method of claim 49 further comprising:

configuring access rights to the digital communication;

enforcing said access rights by managing access to the digital communication and controlling the manipulation of its contents.

51. (Original)   The method of claim 49 wherein the access rights include:

forwarding the communication;

replying; and

replying with carbon copies to pre-selected recipients.

52. (Original)   The method of claim 49 wherein the communication includes an address portion and a content portion, and wherein the access rights include:

copying of the contents of the communication;

cutting the contents of the communication out of the communication and pasting the cut out contents into another location.

53. (Previously Presented)   The method of claim 49 further comprising creating a privilege profile, the profile containing the privileged distribution list and the access rights.

54. (Original)   The method of claim 49 wherein the program is configured to execute automatically and attach the executable module to particular communications according to predetermined selection criteria.

55. (Previously Presented)   The method of claim 49 further comprising displaying a confidentiality notice to a user and requiring that the confidentiality notice be acknowledged by the user before the privileged communication is displayed.

56. (Original)   The method of claim 49 further comprising applying an encryption technique to the digital communication.

57. (Currently Amended)   A method for creating a privileged digital document, comprising the steps of:

creating an executable module which instructs a computer to maintain confidentiality in communication of the privileged digital document to which the executable module is attached by restricting access to the digital document and managing manipulation of its contents, according to an associated privileged distribution list;

attaching the executable module to the document, whereby the executable module instructs the computer to restrict access to the document according to the associated privileged distribution list.

58. (Original)   The method according to claim 57, further comprising the step of executing the executable module when the document is opened.

59. (Original)   The method of claim 57, wherein the document is an encrypted document, and wherein the executable module is configured to instruct the computer to decrypt the document if a predetermined condition is met.

60-70. (Canceled)

71. (Currently Amended)   A digital communication system to comprising:

~~a processor; and~~

a <u>first</u> memory containing a program executable by ~~the Processor~~ <u>a processor</u> to:

attach a privileged attribute to a digital communication;

<u>a second memory containing a program executable by a processor</u> <u>to:</u>

restrict access to the privileged digital communication to an intended recipient and ~~the~~ pre-registered designees of attorney recipients <u>in accordance with the privileged</u> <u>attribute</u>; and

store the privileged digital communication in a segregated location for privileged digital communications on a data storage device.

72. (Currently Amended)   A digital communication system comprising:

a processor; and,

a memory containing a program executable by the processor ~~to~~ attach an executable module to a digital communication, the executable module constructed and arranged to:

restrict access to the digital communication <u>to which it is attached</u> to an intended recipient and pre-registered designees of attorney recipients;

restrict routing of the digital communication <u>to which it is attached</u> to the intended recipient and pre-registered designees of attorney recipients.

10